WHAT IS CLAIMED IS:

1. A hand-held mobile field device configured to provide wireless communication with a plurality of patient medical monitoring devices.

2. The mobile field device of Claim 1 further comprising an accessory interface.

3. The mobile field device of Claim 2 wherein the accessory interface is configured to provide wireless communication between the mobile field device and fixed inpatient room diagnostic units and continuous monitoring systems in patient rooms.

4. A mobile field device in accordance with Claim 1 further configured to provide patient medical diagnoses, personal digital assistant functionality, and net research and access.

5. A network including at least one mobile field device configured to provide communication with a plurality of patient medical monitoring devices, the network being configured to aggregate and to make available to the mobile field unit, a combination of manual, automated, fixed continuous and mobile patient monitoring and assessments.

6. A network including at least one mobile field device configured to provide communication with a plurality of patient medical monitoring devices, and the network electronically connected to databases maintained by a hospital.

7. A network in accordance with Claim 6 further comprising at least one electronic medical library database that distributes reference materials including textbooks, reference materials, periodicals, and medical research electronically, and wherein the mobile field device is configured to display the distributed reference materials.

8. A network in accordance with Claim 6 used to electronically link medical, nursing, residents, fellows, and administrative students with a school's intellectual property materials, general medical references, and periodicals.

9. A network in accordance with Claim 6 in which mobile field devices are used by health care consumers to electronically access medical information, drug information, and for self-monitoring as prescribed by a physician.

10. A network in accordance with Claim 6 wherein the databases utilize a plurality of formats and protocols, and wherein security of communication is provided by format-dependent encryption algorithms.

11. A network in accordance with Claim 6 configured to consolidate input by physicians, nurses, medical research/clinical personnel, and general medical staff, and to send the consolidated input to a member of the group consisting of administrative information databases, patient account records, insurance companies, hospital medical centers, health care information databases, and combinations thereof.

12. A network including at least one mobile field device configured to provide communication with a plurality of patient medical monitoring devices, the network further comprising a central repository containing medical information and a plurality of subsystem databases linked to the central repository via at least one member of the group consisting of encryption software and secure hardware that tags transmissions and retrievals.

13. A network in accordance with Claim 12 linking payment flow information between diagnostic related groups' patient hospital charges and third party insurance providers.

14. A network in accordance with Claim 13 wherein security is provided biometrically.

15. A network in accordance with Claim 14 wherein the biometric security comprises fingerprint recognition.

16. A network in accordance with Claim 12 configured to provide secure patient information electronically on at least one of a local area network (LAN) and a mobile wireless network.

17. A network in accordance with Claim 16 configured to disseminate pathology results and medical research to selected individuals.

18. A network including at least one mobile field device configured to provide communication with a plurality of patient medical monitoring devices, the network configured to link a prescription drug order processing system with prescription data and secure patient documentation and health assessment.

19. A network in accordance with Claim 18 linking pharmaceutical companies, retailers, wholesalers, physicians, and nurses.

20. A network comprising:

a medical database;

a secure medical database monitoring system communicatively coupled to the medical database; and

a first data monitoring manager communicatively coupled to the secure medical database monitoring system;

wherein at least one of the secure medical database monitoring system and the data monitoring manager is configured to provide controlled electronic access to the medical database by a plurality of entities in accordance with a specification provided by an authorized user.

21. A network in accordance with Claim 20 configured to control said electronic access with respect to a patient's data is controlled sequentially, so that at least a first predetermined entity must access the patient's data before a second predetermined entity is permitted access.

22. A network in accordance with Claim 21 further configured to selectively control portions of a patient's data, so that each accessing entity has only a predetermined, limited access to preselected portions of a patient's data, the preselected portions varying dependent upon the accessing entity.

23. A network in accordance with Claim 22 further configured to provide a plurality of threads of accessing entity sequences.

24. A network in accordance with Claim 23 further configured to condition access to a portion of a patient's data upon prior access by more than one different entities.

25. A method for communicating medical data comprising communicating medical data wirelessly to a hand-held mobile field unit from a plurality of patient medical monitoring devices, and communicating the medical data received from the hand-held mobile field unit to a medical database via a secure network.

26. A method in accordance with Claim 25 further comprising wirelessly communicating between the mobile field unit and fixed inpatient room diagnostic units and continuous monitoring systems in patient rooms.

27. A method in accordance with Claim 25 further comprising aggregating, and making available to the mobile field unit, a combination of manual, automated, fixed continuous and mobile patient monitoring and assessments.

28. A method in accordance with Claim 25 further comprising electronically communicating information from databases maintained by a hospital to the mobile field unit.

29. A method in accordance with Claim 28 further comprising transmitting encrypted data from the databases to the mobile field unit.

30. A method in accordance with Claim 25 further comprising electronically consolidating input from physicians, nurses, medical research/clinical

personnel, and general medical staff, and electronically transmitting the consolidated input to a member of the group consisting of administrative information databases, patient account records, insurance companies, hospital medical centers, health care information databases, and combinations thereof.

31. A method in accordance with Claim 25 further comprising electronically linking payment flow information between diagnostic related groups' patient hospital charges and third party insurance providers.

32. A method in accordance with Claim 31 further comprising providing biometric security for the electronic linking.

33. A method in accordance with Claim 32 wherein the biometric security is provided by fingerprint recognition.

34. A method in accordance with Claim 25 and further comprising limiting electronic dissemination of pathology results and medical research to selected individuals.

35. A method for controlling access to a medical database comprising:

defining an access protocol for entities accessing patient data, including at least a first entity having initial access to the patient data;

permitting access to the patient data by the at least first entity;

conditioning each further access to the patient data by additional entities upon prior access by at least one predetermined prior entity.

36. A method in accordance with Claim 35 further comprising conditioning at least one of the further accesses to the patient data upon prior access by a plurality of predetermined prior entities whose accesses are not dependent upon each other's access.

37. A method in accordance with Claim 35 further comprising controlling access to the patient data using biometric and electronic security.